Refinement of Supply and Demand Model for Vulnerability Black Market

Jaziar Radianti*)
(jaziar.radianti@uia.no)

Eliot Rich
(e.rich@albany.edu)
School of Business, University at Albany
State University of New York
1400 Washington Avenue
Albany, NY 12222

Jose J. Gonzalez **)
(jose.j.gonzalez@uia.no)
*) and **) Security and Quality in Organizations
University of Agder, Service Box 509
4898 Grimstad, Norway

2010 International System Dynamics Conference
Seoul, South Korea

Refinement of Supply and Demand Model for Vulnerability Black Market

Abstract: Vulnerability black markets (VBMs) are sites for trading malicious tools targeting software vulnerabilities, from known and patched ones. VBMs enable different actors to access malware and use them to attack vulnerable computers. This article discusses economic reasons that could cause continuity of VBMs. It is assumed that buyers and sellers' decision to trade in the black markets depend upon their perceived costs and benefits. As long as the expected utilities of engaging in the black markets are higher than the costs, buyers and sellers will continuously trade in VBMs. A system dynamics (SD) model is developed to capture such problem. Concepts from market-for-crimes theories are adopted into the model, since they provide a useful perspective for explaining criminal behavior such as in VBM.

Two scenarios are developed for simulating and testing different policies: to limit the opportunities for illicit involvement in VBMs and to introduce stricter law enforcement for discouraging participants from engaging in black market. The simulations show that unless the disruptions toward VBM forums are strong enough, sporadic shut-down only halt their activities temporarily. Stricter law enforcement may be effective to cause the participants discontinuing their activities, if the punishment increases the "price" of involvement in the VBMs.

Key Words: Black market, Software vulnerability, Market-for-crime, System dynamics, Simulation

1. Introduction

The software vulnerabilities markets, including the black markets, have been the subject of numerous discussions and systematic research (Franklin et al. 2007; Miller 2007; Sutton et al. 2006; Zhuge et al. 2009). The research covers a wide range of perspectives—theoretical, modeling and empirical research. The most easily observable black markets appear online, operating in the Internet Relay Channels (IRCs) and underground websites. The emergence of these markets is important, since they may have a costly impact on computer-based environments.

The question arises whether running vulnerability black markets (VBMs) is an illegal activity or not. Chiplin (1985) asserts that criminal attribution to the black economy depends upon the law in a particular country. Judging the legitimacy of any activity in cyberspace is even more difficult than traditional crime, since the illegal activities might be hidden, cross line of jurisdiction, or beyond the reach of existing laws. These markets trade malicious code such as exploit kits, malware, obfuscators, botnets, spamming and denial of service attack tools, in addition to credentials and financial information. Anderson et al. (2009) argue that, according to some countries' laws, the VBM type of business may not be illegal, but it may become illegal when the exploits from such trades are deliberately used for attacking computers of potential victims. From this

perspective the illegality of the VBM activities becomes apparent. Hence, I assume in this paper that the main source of VBM illegality is the use of traded tools by malicious agents for illegal purposes.

Legal efforts to shut down hacker websites and catch the main players have been made. However, the cyber world is spacious, allowing hackers to vary their malicious activities. Sporadic legal action against their malicious websites does not seem to fully solve the VBM problem. Several questions arise: What factors are motivating black market sellers and buyers to continuously engage in such illegal activities? What sort of incentives or disincentives should be used to limit or discourage them from further activity in the black market? What are the effects of particular incentive measures on supply and demand of malicious tools in the black markets?

Economic theories have been used to explain and analyze criminal behavior and provide rewarding perspectives to answer the questions addressed in this article. Chiplin (1985) mentions the limitation of economic analysis to answer *what-if* or *trade-off* type questions, the effects of particular choices on observed variables. On the other hand, there is a modeling method, system dynamics (SD), which enables one answering *trade-off* and *what-if* type questions, thus overcome such limitation in economic analysis. SD is a computer-aided modeling method that enables researchers to vary the assumptions of the model and examine behavioral impacts over time after changes are made through a set of simulations. A SD model on VBM has been developed in earlier studies (reference to be added), but a part of the model, i.e. the exploit supply and demand in black markets, requires further improvement as I explain is Section 2.2 later.

The purpose of this paper is threefold: adopting the market-of-crime concepts to explain the behavior of supply and demand of illegal activities in the online black markets; transferring these concepts and proposed policies to control the decision to involve on illegal activities into a simulation-enabled SD model; and, observing the change in the supply and demand behavior of such online market over time, as well as testing the hypotheses on the impact of different policies on the availability of malicious tools in the online black markets.

2. Literature

2.1. Economic Approaches: “Black Market” vs. “Market for Crimes”

Black market supply and demand in the economic literature is mostly discussed as a regulated market under perfect and imperfect competitions (Boulding 1947, Plumptre 1947, Bronfenbrenner, 1947, Michaely 1954; Gönensay 1966). In this context, black market refers to the transactions taking place below or over the regulated price. These theories treat the black market as a result of the pre-determined price for a particular commodity—a common practice after the Second World War in the United States.

The “black market” label attaches to the case under study (VBM). However, this market behaves as an unregulated market instead of a regulated market. In addition, to analyze

the supply and demand in a VBM based on actual price is tricky. Different "price setting" is required to analyze the case.

Different economic approaches have been widely used to explain the supply and demand for crime and punishment (Becker 1968; Chiplin 1985; Ehrlich 1996), decision to participate in illegitimate activities (Ehrlich 1973), and organized crime (Garoupa 2000). The recent work of Eeten and Bauer (2008) embraces security decisions, incentives and externalities in the "economics of malware" framework.

Becker (1968) is one among many who makes use of modern economic analysis to study crime issues. Becker uses a model of decision making to engage in criminal activities and the link between crime and punishment. The summary of studies in this field can be seen in Table 1.

Table 1. Studies Using Economic Approaches to Crime

Author(s)	Focus	Theoretical approach	Economic analysis
Eeten & Bauer (2008)	Market of crime and Market of security	Externalities, Asymmetric information	Marginal analysis (Marginal benefits of crime and security, Marginal costs of crime and security)
Garoupa (2000)	Organized crime market	Criminal organization as a vertical structure that extorts rents from agents	Competitive vs. monopolistic criminal market (extortion, violence, political corruption)
Ehrlich (1996)	Market for offences	Decision-theory-under uncertainty	Equilibrium analysis, cost-benefit analysis
Chiplin (1985)	Offences and probability of detection	Decision-theory-under uncertainty	Probability of detection, size of punishment and availability of opportunities are determinants of the offence rate; cost-benefit analysis
Ehrlich (1973)	Participating in illegitimate activities	Decision-theory-under uncertainty	Response of offenders to incentive and decision to commit crime; Econometric
Becker (1968)	Market for offences	Decision-theory-under uncertainty	Marginal cost, marginal revenue and supply of offences, punishment

Incorporating criminal behavior into a market model, optimal crime control policy through negative or positive incentives (those that prevent offenders from pursuing illegitimate activities, or induce participation in legitimate alternatives) are central in these approaches. Economic concepts such as resource allocation, cost-benefit analysis and optimizing choice under various constraints are used in market crime analysis. Uncertainty involved in the criminal activity such as the probability of being caught and the severity of punishment and individual attitude toward risk also becomes a part of the analysis of an individual decision to commit crime.

A comprehensive illustration on an offender's decision to participate in illegal activities can be found in Ehrlich's work (Ehrlich 1973). His contributions go further than just discussing the cost of punishment. He also introduces the concepts of opportunities for both punishment and reward, i.e. costs and gains from the engagement in licit and illicit activities, and links decision-theory-under-uncertainty for optimal resource allocation and select licit-illicit participation. Ehrlich further analyzes the interaction of offense-defense and crime-law enforcement activities.

Chiplin (1985) suggests the *clear-up rate,* i.e. the proportion of reported crimes that has been cleared-up by the police, as an alternative to price setting. Chiplin's work focuses on the determination of the number of offences and the importance of punishment as a deterrent. Cost-benefit analysis and optimal punishment are added to analyze the public policy formulation, the offender's behavior and optimal response by legal authorities.

Ehrlich (1996) proposes a market model of crime where all relevant actors are assumed to follow optimizing behavior. Instead of conceptualizing the market for offence as a "physical" meaning, Ehrlich (ibid) uses an abstract theoretical Walrasian market, i.e. assumes that the aggregate behavior of suppliers and demanders is coordinated and made mutually consistent through adjustments in relevant prices. Market equilibrium occurs as an interaction between offenders and law enforcers, although it is possible to include other parties such as consumers of illicit goods and potential victims.

Garoupa (2000) examines optimal law enforcement in the presence of organized crime—an organization with special properties such as economies of scale and exploitation of monopolistic pricing on the supply of illegal goods and services, practicing violence against other legal and illegal businesses, and avoiding resource dissipation through competitive lobbying and corruption. Garoupa points out that the presence of a dominant firm-like criminal organization (e.g. Mafia) extorting smaller criminal firms is missing from policy discussion for the current market of crime literature. Garoupa (ibid, p.287) concludes that in the presence of organized crime, the optimal enforcement policy is one of less severity rather than more. Garoupa bases his arguments on the observation of vertical integration in the world of criminal activity that creates entry barriers and makes criminal offences less probable and/ or attractive. The author also suggests that the government policy should be more severe in a monopolistic criminal market than in a competitive one.

Van Eeten and Bauer (2008) touch on the malware issue as a part of cybercrime and cybersecurity in the market of crime concepts by using marginal analysis. They assume that security violations occur at increasing cost. The marginal benefits of additional security violations are a decreasing function of the level of violations. Technological change enables less costly malware production and thus expands the supply of crime. Reduced marginal costs of security violations lower the marginal costs of crime and produce higher level of security violations and vice versa. In the market for security, a higher level of security can only be achieved at higher marginal costs. Change the costs of providing security, and the benefits of having security will shift the marginal costs and benefits. Reduction of the costs of security results in a higher security level. This work focuses on incentives and disincentives that influence the individual/organizational decisions to undertake measures that mitigate the costs associated with the spread of malware.

Although both black market and market for crime concepts employ different analyses and approaches to explain supply and demand, there are similarities in perceiving the problems. *First*, economists mostly regard illegal activities as incentive failures, whether as a result of information asymmetry or externality. *Second*, security and protection from being victim of crime are considered as both a private and public good.

However, private protection is limited compared to the security provided by the government through deterrence, law and punishment. Hence, socially optimum policy is needed. *Third*, in absence of moral reproach, proposals to solve illicit activities include using legal measures e.g. police surveillance, fines, and imprisonment.

This work is an attempt to find the best way to explain the dynamics of supply and demand in the online black markets that trade malicious tools for exploiting software vulnerabilities for launching attacks on unprotected systems. From earlier reviews of economic theories, I conclude that the market-for-crime approach better explains the supply and demand of exploits in the VBM due to the similar properties between these two markets. The VBM also behaves as an unregulated market. There is neither a pre-determined price that dictates the black market supply and demand, nor tax avoidance (sales or excise) issues to make it a "black market". Hence, this work hypothesizes that the supply and demand behavior of the VBMs is similar to a market for crime. Prior to presenting a dynamic model that merges the market-for-crime concepts to explain the online vulnerability black market case, a brief review of the works combining economic market theory and system dynamics is presented here.

2.2. System Dynamics and Market Modeling

System dynamics (SD) is a methodology for modeling the dynamic of systems representing real world issues. SD captures non-linearity and time delays, feedback loops and their interactions in complex systems. Outputs of SD modeling include influence diagrams, causal map analyses and simulations that allow different agents to learn how to manage complex systems. The typical SD problems will involve quantities which change over time and can be described in terms of graphs of variables over time (Coyle 1996; Richardson et al. 1981).

SD has been widely used to analyze economic issues. Most economic problems have dynamic features by nature and contain feedback loops and quantities that change over time. A market is a good example of an economic phenomenon that contains self-regulating mechanisms or balancing loops as central issues in the dynamic modeling. A market that works through supply, demand and price can be simply represented as in Figure 1.

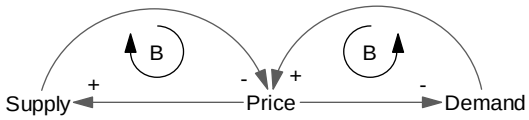

Figure. 1
Simple Loop of Supply and Demand

Meadows' commodity production cycle model (1970) is a prominent example of an SD market model. Sterman (2000) improves the model by proposing the generic commodity market that is regulated through price. If inventory coverage increases, the price will fall down. Shortage in inventory coverage will increase the price. The firm's supply is determined by capacity acquisition and capacity utilization. Sterman (2000)

argues that price serves as market self-regulation, but that there are also market price-like concepts that work as self regulating agents such as quality and availability.

There are two SD-VBM model proposals so far: *first*, a VBM model that incorporates decision making theory under uncertainty (Reference to be added, 2007), and *second*, an exploit supply-and-demand model that captures how the market operates in the real world (Reference to be added, 2009).

The *first* SD model assumes that licit or illicit opportunities are available for hackers entering black or legal markets. There are two possible outcomes (expected value) for involvement in each market as a result of the probability of having successful transactions or being caught by the law. One of the weaknesses is that this model assumes such transactions occur as a part of the VBM that I call the *skilled-hacker* market. It is a market that focuses on trading zero day vulnerabilities of leading software products from the first hand discoverer. Although thorough study indicates that such market exists, its obscurity makes this type market difficult to be investigated further. Thus, the model does not have enough empirical support. In addition, how the "price" is captured in the model and regulates the market is not yet clear

The *second* SD-model views the black market as online sites where illicit goods are traded. The black market owner regulates the inflow of traded goods, while the potential buyers' attraction depends on the availability of the traded goods in the black market. The role of the black market owner is to ensure that the advertisements are legitimate goods (i.e. not widely known public tools). This is the way the owner keeps the market running—attracting participants with similar interests and making them trust the market. This differs from the commodity market where shortage or excess inventory affects the price. In an online black market, inventory (here interpreted as exploit advertisements) does not directly affect the price (e.g. quantity supplied increases as price rises and quantity demanded decreases as price rises). The supply depends on black hat hackers' willingness to convert available exploits to black market commodities, and the black market staff's capacity to select and verify the malicious tool advertisement. Capturing the production of exploits through the black market owner's decision weakens the market notion in the model. There is a "price"-like concept dictating supply and demand in the black market, but not in terms of a monetary measurement.

The SD-model in this article aims at improving or refining the exploit supply and demand in the black markets so that it conforms more closely to an unregulated market operation. The market-for-crime literature offers ideas that fit the actors' behavior in the online black markets. I adapt a generic SD commodity model from Sterman (2000, p. 798-823) to improve this model. In the proposed model, the market makers continuously involve themselves in online black markets according to their perceived costs and benefits. Hence, the *Black Market (BM) involvement price* serves as a self-regulating mechanism that determines the involvement decision. This model will be presented in Section 3.

2.3. Hypotheses

One of the questions addressed in this paper relates to the type of incentives or disincentives that can be used to affect the decisions of relevant parties to become involved in online black market activities. To test the hypotheses developed in this study, model simulations will be used. Two sets of policies will be tested using the model: to limit the opportunity for all participants to be involved in online black markets (*Policy 1*); and to increase the severity of punishment through tighter law enforcement (*Policy 2*). Further explanation of this policy in the model is described in Section 4. Hypotheses is developed in this study, that the availability of exploits in the black market due to the application of policy to *prevent* individuals from engaging in illegal activity or due to the application of policy to *punish* individuals that engage in illegal activity.

3. The Model

In this paper, I borrow Ehrlich's concept (1996) who regards the market-for-crime as an interaction between the offenders (who commit or supply the crimes) and defenders (who demand protection against the crime). Crime supply is affected by the cost and benefit of such action and is evaluated by a net return per offence. Net return has to be higher than a given threshold before the individual decides to engage in criminal behavior. The offender's direct costs include the probability of conviction and penalty if convicted. They are also affected by private and public demands to obtain protection from crime. Demand for private protection from potential victims is a combination of self-insurance and self-protection, while demand for public protection is achieved through optimal law enforcement and crime control. Ehrlich states that the market equilibrium is reached when the relevant actors do not need to adjust their behavior and alter the prevailing net return or price associated with crime (e.g. *criminals* look at the next expected return from crime, *private individuals* look at their risk and cost of victimization, and *government* looks at the relevant social welfare function).

In modeling this online black market case, a few assumptions are made. The demand does not originate from the potential victims that need security protection. The demand only comes from the potential black market buyers that search for malicious tools. Both black market suppliers and potential buyers are maximizing their utilities. As long as the expected utilities or benefits of engaging in the black markets are higher than their threshold (costs of their effort), the market makers will continue to buy or produce malicious tools. Hence, buyers in BM look at expected utility from buying malicious tool in BM, while sellers in BM look at their next expected benefit from involving in BM.

Figure 2 is a stock and flow diagram of the supply and demand in the black markets. The price setting process to adjust supply and demand of exploits in the black markets adopts a similar process for the commodity market as proposed by Sterman (2000). The italic words in the rest of this paper indicate the name of variables in the model. Note that the "exploits" term in the model is only a simplification to capture various malicious tools such as viruses, malware, obfuscators, etc., that are commonly advertised in the online black markets.

The diagram contains four loops that balance the supply and demand in the black markets: *Supply Responses* (B1), *Demand Responses* (B2), *Buyers' Effect* (B3) and *Goal Adjustment* (R1). The stock of *Exploits in BM* increases as the inflow *Supply for Exploits in BM* increases, and depletes as exploits are outdated or purchased. *Demand* and *Supply for Exploits in BM* depends on the *BM Involvement Price* that in this model is regarded as "price setting".

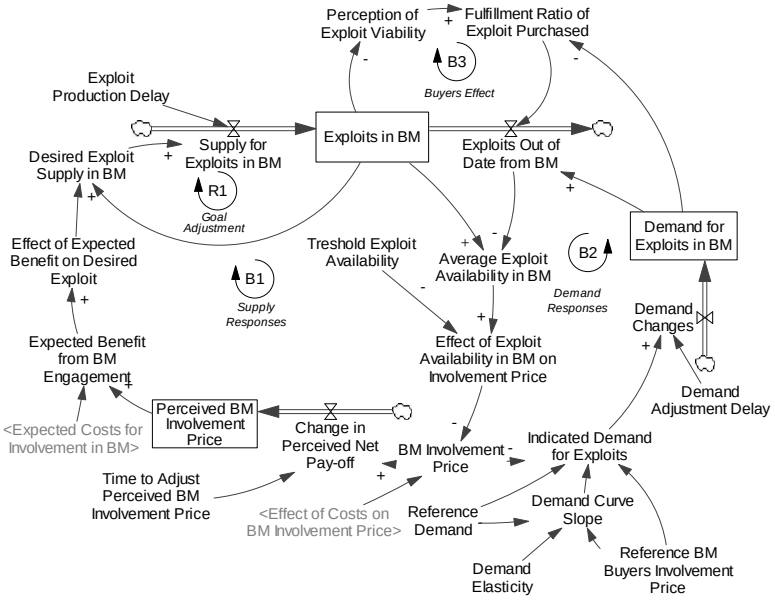

Figure 2. Supply and Demand for Exploits in the Black Market

On the *Supply Responses* loop (B1), higher *BM Involvement Price* leads to higher *Perceived BM Involvement Price*. The *Desired Exploit Supply in BM* is a reaction to *Expected Benefit from BM Engagement.* The *BM Involvement Price* depends on *Exploits Availability in BM*, i.e. the balance of supply and demand. The current supply is the available exploits in the black market. Demand is captured by exploits that are outdated from the black market. *BM Involvement Price* tends to rise when *Average Exploit Availability* (the ratio of exploits in black market to those that are outdated) falls. Price is what black market sellers "pay" for supplying malicious tools. It includes the risk of being caught by law enforcement, prospective loss of being cheated by other BM players (e.g. buyers do not pay), and prospective loss in value of the offered tools when they are known by the public. The price rises because there is less competition for the supplier offering malicious tools. Fewer competitors make active sellers bear a higher risk, since they are much easier to identify.

The Buyers' Effect loop (B3) determines the viability of the exploit outflow. *Fulfillment Ratio of Exploit Purchase* captures a ratio of *Perception of Exploit Viability* and *Demand for Exploits*. If there are no exploits available in the black market, demand cannot be met and there are no outdated exploits. Most commodity market models use "capacity to use" and "capacity to produce" that affect the inventory. This model

(Figure 2) uses only *Desired Exploit Supply* and *Exploit Production Delay* to determine the exploit supply, such as captured in the *Goal Adjustment* loop (R1). Black market sellers increase the desired exploit supply when agents perceive that the benefit of the activity is greater than the cost. Thus, the black market still remains attractive to black market suppliers.

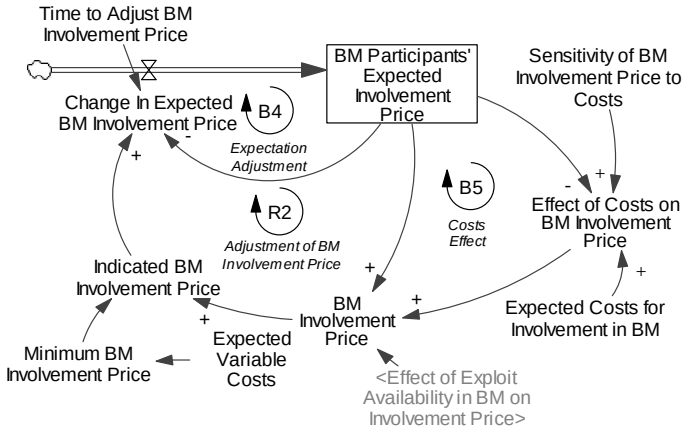

Figure 3
BM involvement price formation to adjust supply and demand for exploits

Demand Responses loop (B2) captures demand for exploit behavior. This model assumes that the demand comes from potential buyers who are willing to purchase the malicious tools in the black market. Black market buyers presumably arrive at their price from the usefulness of the malicious tools being bought in the black market and their risk of being cheated by dishonest sellers. For buyers, their price increases as they encounter frequent dishonest sellers or discover that the malicious tools they are purchased are useless. Therefore, *Demand for Exploits in BM* falls when the *Indicated BM Involvement Price* rises. Formulation of *Indicated Demand for Exploit* follows Sterman (2000, p. 812) as a response to *BM Involvement Price* relative to *Reference BM Buyers' Involvement Price.* An assumed linear market demand curve is also applied in this black market case.

Sterman (2000, p. 814) specifies that the price formulation in economics is mostly described as an equilibrium price, adjusted by a function of current demand/supply balance. The price setting in this model is interpreted as the *BM Involvement Price* of different actors in the market—an integration of the perceived benefit from supplier and buyers. The *BM Involvement Price* formation is modeled in Figure 3.

The process of price discovery is modeled by Sterman as a formation of expected level price by market participants that will clear the market. The price formation in this black market model is that the black market participants form expectations about relative benefits and probability of punishment as a link to subjective expectation and objective opportunity. Erhlich (1996, p. 46) suggests the expected net return per crime is equal to [`the expected gross payoff–direct costs incurred in acquiring the loot–forgone wages from legitimate activity–(probability of conviction)x(prospective penalty if convicted)`].

I have already mentioned that the price concept for this black market case, i.e. net return of perceived benefit, compares to perceived risk of each player—buyer and seller. The change in the actual net return from criminal activities can thus exceed or fall below the threshold level of marginal offenders and affect the actors entering or exiting from such activities.

If actual *BM Involvement Price* exceeds the current belief about the equilibrium *BM Involvement Price*, black market participants will adjust their expectation of the price until it reaches the market-clearing price level. Adjustment in the actual *BM Involvement Price* is a black market players' response to the belief about the *Costs of Involvement in Black Markets*, and the exploit supply and demand balance. The expected price adjusts to the *Indicated BM Involvement Price.* In this black market model, *Indicated BM Involvement Price* is assumed to be equal to the *Minimum BM Involvement Price*. It is affected by the *Expected Variable Costs of BM Involvement.* Variable costs as a result of different market players' decisions to intensify or lessen black market activities are excluded from this model. Hence, *Expected Variable Costs of BM Involvement* is a constant value.

In the market-for-crime concept, equilibrium is achieved when every actor does not need to adjust their expectation any longer by looking for the next expected return from their black market involvement. To equilibrate this BM supply and demand model, the *Expected Variable Costs, Expected Costs for Involvement in BM, Reference Demand* and *Reference BM Involvement Price of BM Buyers* are set as constant. Initial parameters in the model are as follows:

Table 2. Initial Parameter Values in the Model

Parameter	Value	Unit
Sensitivity of BM Involvement Price to Costs	0.5	dimensionless
Time to Adjust BM Involvement Price	1	month
Exploit Production Delay	1	month
Desired Exploit Coverage	1	month
Demand Elasticity	0.5	dimensionless
Sensitivity of Exploit Coverage to BM Involvement Price	1	dimensionless
Time to Adjust Perceived BM Involvement Price	1	month
Demand Adjustment Delay	1	month
Max Demand	∞	exploits/month

4. Results, Analysis and Insights

This part will present the simulations using the model that has been explained in Section 3. The simulations are intended to test several conditions that apply to the model and to see how it reacts to parameter changes.

4.1. Base Run

The initial model was set as equilibrium. Thus, *Supply for Exploits in BM, Demand for Exploits in BM, Reference Demand* and *Reference BM Involvement Price, Expected Costs for Involvement in BM* and *Expected Variable Costs,* are all equal with an initial value of 150. Figures 4a and 4b show the simulations of the supply and demand for

exploits behavior, when parameter changes in the model were made, i.e. the *Reference Demand* was increased in month 10, *without* and then *with* the changes in *Demand Adjustment Delay* and *Time to Adjust Perceived BM Involvement Price* (Table 3). Other parameter values in the model were left unchanged.

Table 3. Parameter Changes in the Base Runs

Parameters	Equilibrium	Base	Slow Adjustment
Reference Demand	150	Step 10, t_{10}	Step 10, t_{10}
Time to Adjust Perceived BM Involvement Price	1 month	1 month	1.2 month
Demand Adjustment Delay	1 month	1 month	1.5 month

Note that the parameter change did not cause the demand in Figure 4a (thin line) to immediately increase to the new demand. It was adjusted gradually—increasing in month 11 by approximately eight percent, and reached its peak value of 163 in month 19. The supply for exploits in Figure 4a (thick line) responded slower, but increased faster than the demand change. It began to go up at month 12, peaked at 166, and then went down to 155 as the demand reached its highest peak. Both supply and demand for exploits oscillated for 38 months and reached a new equilibrium value of 160.

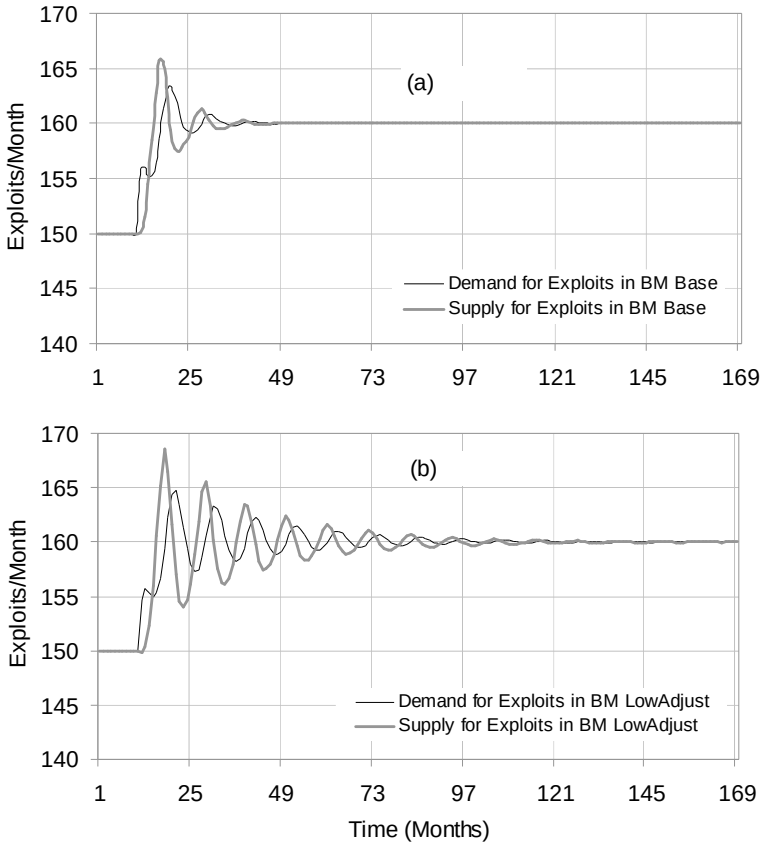

Figure 4a and 4b. Simulation Supply and Demand for Exploits

Figure 4b shows the same supply and demand for exploits, but the market makers took longer delay to respond to the change in demand. The longer adjustment process in supply and demand prior to the new demand/supply equilibrium is indicated by a longer oscillation along the supply and demand graphs over time. This basic simulation shows how the adjustment process caused by lag in perceiving the system alteration takes place. A similar principle would be used as a basic explanation for the next policy tests.

4.2. Policy Tests

The policy tests are intended to examine two scenarios; to develop disincentives by removing the opportunity to be involved in the black markets for all types of participants (*Policy Test 1*) and, by introducing stricter law enforcement and severity of punishment for any malicious online activities (*Policy Test 2*). The base simulation (Figure 4a) is used as a starting point for further simulations. The purpose of these policy tests is to assess the effect of the aforementioned disincentives on diverting market players from continuous online black market engagements.

Policy Test 1 deals with disturbing the opportunity for entering the black market forums through internal disruptions (temporarily downtime) or longer and permanent downtime. The latter might be conducted deliberately by external enforcement agents, such as Operation Firewall that successfully shut down the black markets for fraudulent cards and botnet sites and terminated the operation of the targeted sites (See www.secretservice.gov). The disruption policy test was implemented by inserting the Pulse Train function to the *Exploit Production Delay* parameter in the model. This function allows a modeler to "disturb" the delay, its duration and repeated times. The normal exploit production delay in the model that ascertains continuous exploit supply is one month. Three scenarios of disturbance were developed—short, medium and long down time. The parameter changes are specified in Table 4:

Table 4. Parameter Changes in *Policy Test 1*

Parameters	ShortDownTime	MedDownTime	LongDownTime
Reference demand	Step 10, t_{10}	Step 10, t_{10}	Step 10, t_{10}
Repeated disruption	Every 50 months	Every 50 months	Every 50 months
Duration of disruption	0.5 month, t_{72}	1 month, t_{72}	1.7 months, t_{72}

These changes implied that in the *ShortDownTime* scenario, exploits production delay would be two weeks longer, in *MedDownTime* scenario, the delay would occur a month longer while in *LongDownTime* would be 1.7 month longer than the normal delay. The last value was the minimum duration delay that would cause the exploit supply to begin collapsing. The selection was made by varying the parameter values until a number was found where the observed variable started to decay.

Policy Test 2 is conducted by varying the value of *Expected Costs for Involvement in Black Markets* in the model (*HiCost* scenario) and later also by changing the *Sensitivity of the BM Involvement Price to Costs* (*HiCostsSens* scenario). The parameter changes are summarized in the following table:

Table 5. Parameter changes in *Policy Test 2*

Parameters	HiCosts	HiCostsSens
Reference demand	Step 10, t_{10}	Step 10, t_{10}
Expected costs for Involvement in BM	Step 50, t_{50}	Step 50, t_{50}
Sensitivity of *net pay-off* to Costs	0.5	1

The *Expected Costs for Involvement in BM* are not modeled in a detailed way, and only captured as a constant parameter (see Section 3). Thus higher costs for black market participants are determined exogenously by assigning a higher value for this parameter.

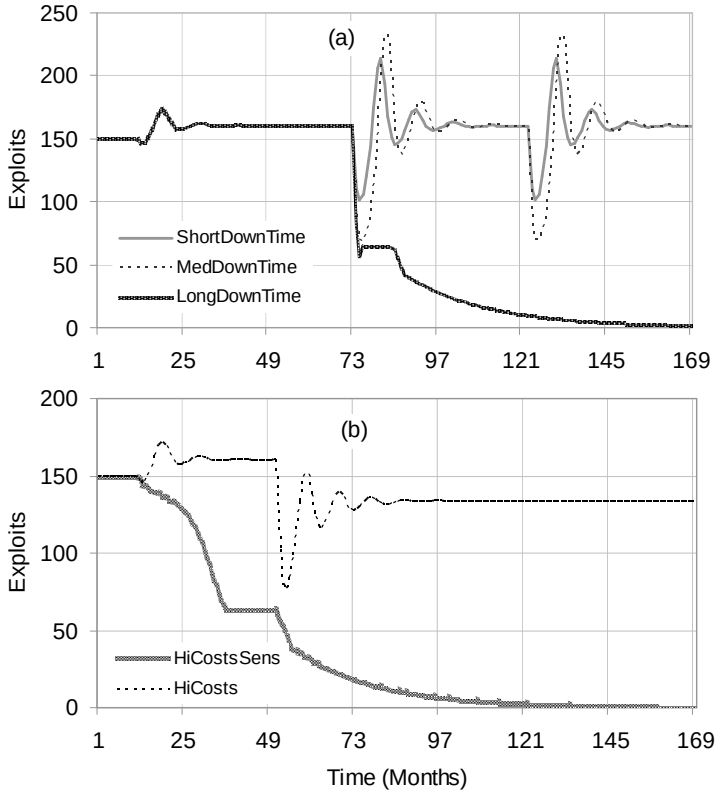

Figure 5a and 5b. Policy Test Results of Exploits in Black Market

Figures 5a and 5b illustrate the simulation results of *Policy Test 1* (disruption of the market operation) and *Policy Test 2* (law enforcement and punishment) respectively. The simulation focuses on the behavior of the *Exploits in Black Market* variable. *ShortDownTime* (grey, thick-line) and *MedDownTime* (dotted, thin-line) simulations are drawn in Figure 5a, two disturbances occurred in month 72 and 152, after the market was able to adjust the increase in the demand for exploits in month 10. In both scenarios, the *Exploits in Black Market* returned to its "normal balance" value of around 160. The differences of the results in these two scenarios are shown in the length and the height of oscillations. *The ShortDownTime* scenario resulted in shorter and lower oscillations than the *MedDownTime* scenario. This indicates that a longer *Delay in Exploit Production* might decrease the system's ability to return back to its normal black market operation. The *LongDownTime* scenario (black, thick-line) caused the observed variable to decrease over time, and was completely incapable of returning to its normal market activities, even falling to zero around month 151.

Figure 5b is the simulation results from the scenario of higher costs to be involved in the black market. The increasing costs could originate from the possibility of participants being caught and jailed by law enforcement or loss of legal opportunities because of participation in riskier black market activities. The *HiCosts* scenario (dotted thin-line) assumes that the law enforcement is stricter than usual and that hence the costs of black market participation will increase. Unlike the earlier *HiCosts* scenario where the *BM Involvement Price* alteration did not affect costs, in the *HiCostsSens* scenario (dashed, thick line) the *BM Involvement Price* did influence cost. A maximum value of one was given for this scenario.
The differences in the behavior between the two scenarios are apparent. The *HiCosts* scenario caused the *Exploits in Black Market* to fall in month 50 before oscillating over time and settling at a new equilibrium value of 133, around month 93. It decreased approximately 16 percent from the previous equilibrium value. The *HiCostsSens* scenario showed that the exploits in the black market gradually depleted from month 50 to 97, and then quickly fell to zero around month 120.

Although the number of exploits in the black market went down, the supply and demand for exploits did not follow the adjustment process. Thus, as the supply continued to decrease, the demand for exploits went up and ultimately leveled off as the supply dropped to zero. The simulation results of supply and demand in *Policy Test 2* for the two scenarios above are shown in Figures 6a and 6b.

There two feedback loops—The *Goal-Adjustment* loop (R1) and the *Supply-Response* loop (B1)—that are responsible for the supply behavior. There is a correction mechanism (Figure 3) in the *Goal-Adjustment* loop such that when the number of *Exploits in the Black Market* goes down, the *Desired Exploit Supply in BM* will likewise decrease. The *Supply-Response* loop also affects this behavior as *BM Involvement Price* and *Perceived BM Involvement Price* go down. Unless the expected benefit from black market engagement is higher that the expected costs, the supplier would not produce malicious tools.

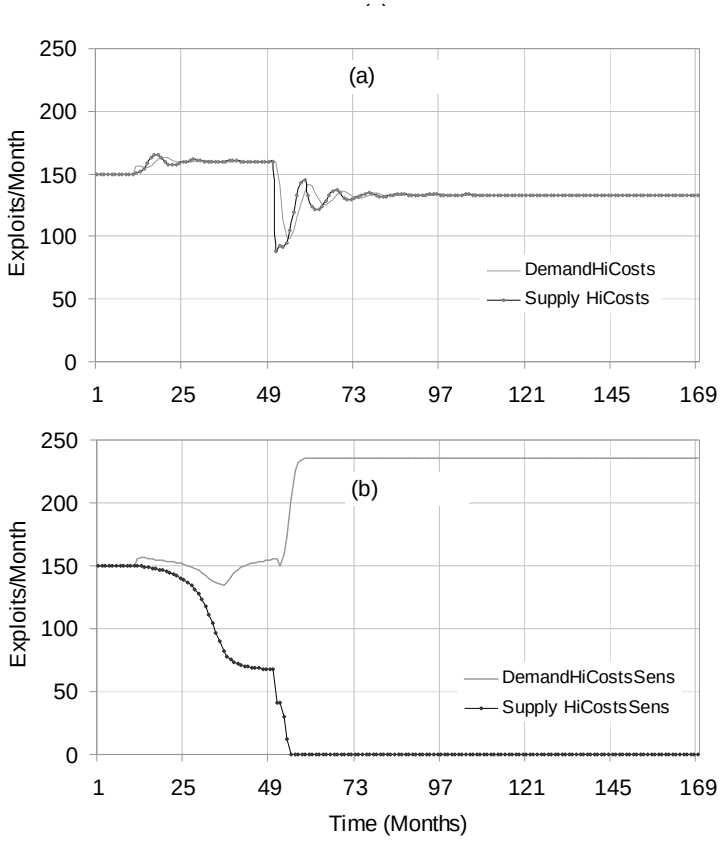

Figure 6a and 6b. Supply and Demand for Exploits at Higher Costs

4.3. Insights

Experiments with the model using two disincentives, i.e. closing the opportunity to enter online black markets and tighter enforcement have provided some insights. If the concern of the security community is to diminish illegal activities in cyberspace such as the black market for vulnerabilities, experiments with the two policies shows that they are basically able to do this.

However, by using the existing assumptions in earlier simulations, there are differences in the stages to reach the goal for diminishing black market activities. In *Policy Test 1*, the experiments show that the duration of the black market forums' disappearance is the main reason for black market activity to lessen, weaken, or completely disappear. With this existing assumptions in the model and all other things being equal, if the extra delays in producing and supplying new malicious tools for the black market is between 0-1.6 months (0<extra exploit production delay<1.6 months), these regular/irregular interruptions only create a fluctuation in the stock of exploits. The longer the delay to supply exploits in the black market, the greater the height of fluctuation. This means that the system has to make harder effort to recover from the disruptions. In reality the recovery process is implemented by the efforts of the forum owners to notify the previous black market members possessing a valid, registered email address and encourage them to use the black market forums again.

Longer extra delay time (in this model > 1.6 months) causes fewer available exploits in the black market. In turn, as the downward process occurs, more sellers are unable to enter the black markets. This reduces the desire to create exploits and will eventually drop the stock of exploits in black market to zero. Such a situation will deactivate the black market forums because many market makers will be reluctant to become involved in online forums with interruptions.

The Policy Test 2 increases the cost of the market makers to be regularly involved in the black market. By increasing the costs around 30 percent and all other things being equal, the fluctuations will occur in market activities. However, the market could still operate afterwards although on a less intensive scale. A few experiments were also conducted by varying the parameter sensitivity of *BM Involvement Price* to the costs. It seems that if the value of sensitivity is between 0.4 and 0.96, the black market can still operate and find a balance between the supply and demand. However, the balance will decline as the sensitivity value increases. For example, at sensitivity 0.96, the stability of the stock of exploits in the black markets decreases to around 60 percent from its initial equilibrium. Sensitivity values between 0.97 and 1 however, cause the market to become completely disrupted and unable to operate. The insights from this analysis is that if law enforcement only increases the cost to the seller, risk-loving participants would still conduct this illicit activities, particularly if the *BM involvement price* equals *BM Participants' Expected BM Involvement Price* and *Expected Costs for Involvement in BM*. If law enforcement were made stricter, it might cause costs to be sensitive to the point of changing the *BM Involvement Price*, and thus market activity would weaken or even fade away.

5. Conclusions

This article addresses several questions listed in the Introduction. The application of the market-of-crime concepts provides an improved method for explaining the online black market supply and demand for malicious tools. *Expected BM Involvement Price* from buyers and sellers in the black markets are a central concept for explaining their motivation to continue or discontinue their illegal activities. To limit the opportunities for illicit engagement and to increase the severity of punishments, two policies were tested in this study. A set of simulations using an SD model were implemented. Using these two policies, significant differences in the behavior of supply and demand in the black markets, and exploit availability were noted. Thus, the simulation tests support the hypotheses set forth in this study. However these two disincentives reveal different processes and effects in before changing the behavior of market participants to continue or discontinue their buying and selling on the black market. In the disruption policy, the duration of the disturbance to the online black market needs to be long enough to discourage the participants' involvement. In the punishment policy, the *Sensitivity of the Costs of the BM Involvement Price* plays an important role in halting the continuous supply and demand for exploits in the black market.

The sources of outdated exploits from black markets are found not only in purchasing but also in targeted software vulnerabilities that are patched. This could be added to the model. The model itself is limited for not elaborating further than it does on the detailed

calculation of costs and benefits of the market players. However, the model has revealed plausible behaviors and trends that are significant enough to derive some valuable insights to learn as noted. This model can be expanded into a broader one to include the life cycle of software vulnerabilities and hackers' decisions to operate between legal and illegal markets.

References

Anderson, R., Böhme, R., Clayton, R., and Moore, T. "Security economics and the internal market," European Network and Information Security Agency.

Becker, G. "Crime and punishment: An economic approach," *Journal of Political Economy* (76) 1968, pp 169-217.

Boulding, K.E. "A note on the theory of the black market," *The Canadian Journal of Economics and Political Science / Revue canadienne d'Economique et de Science politique* (13:1), February, 1947 1947, pp 115-118.

Bronfenbrenner, M. "Price control under imperfect competition," *The American Economic Review* (Vol. 37:1), Mar 1947, pp 107-120.

Chiplin," 1985.

Coyle, R.G. *System dynamics modeling: A practical approach* Chapman & Hall, London, 1996.

Ehrlich, I. "Participation in illegitimate activities: A theoretical and empirical investigation " *Journal of Political Economy*, (81:3) 1973, pp 521-565.

Ehrlich, I. "Crime, punishment, and the market for offenses " *Journal of Economic Perspectives* (10:1) 1996, pp 43-67.

Franklin, J., Paxson, V., Perrig, A., and Savage, S. "An inquiry into the nature and causes of the wealth of internet miscreants," 14 th ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, USA, 2007.

Garoupa, N. "The economics of organized crime and optimal law enforcement," *Economic Inquiry* (38:2) 2000, pp 278-288.

Gönensay, E. "The theory of black market prices," *Economica, New Series* (33:160), May, 1966 1966, pp 219-225.

Meadows, D.L. *Dynamics of commodity production cycles* Wright Allen Press, Cambridge, Massachusetts, 1970.

Miller, C. "The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales," Workshop on Economics of Information Security, Pittsburgh, USA, 2007.

Nordin, J.A., and Moore, W.R. "Bronfenbrenner on the black market," *The American Economic Review* (37:5), Dec, 1947 1947, pp 933-934.

Plumptre, A.F.W. "The theory of the black market: Further considerations," *The Canadian Journal of Economics and Political Science / Revue canadienne d'Economique et de Science politique* (13:2), May 1947, pp 280-282. .

Richardson, G.P., and Pugh III, A.L. *Introduction to system dynamics modeling* Productivity Press, Portland, Oregon, 1981, p. 404.

Sterman, J.D. *Business dynamics: Systems thinking and modeling for a complex world* Irwin/McGraw-Hill, Boston, 2000.

Sutton, M., and Nagle, F. "Emerging economic models for vulnerability research," The Fifth Workshop on the Economics of Information Security (WEIS), Robinson College, University of Cambridge, England, 2006.

van Eeten, M.J.G., and Bauer, J.M. "Economics of malware: Security decisions, incentives and externalities," Organization for Economic Co-operation and Development.

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., and Zou, W. "Studying malicious websites and the underground economy on the chinese website," in: *Managing information risk and the economics of security,* Springer US, 2009.